SECURITY ANALYSIS REPORT

HTTP Security Headers Assessment

Target URL:
https://cyberalphas.com

Scan Date:
August 15, 2025 at 01:03 AM UTC

Overall Security Score:
63/100

Risk Level:
■ **Medium**

Prepared by:
CyberHeaders Security

CONFIDENTIAL

This report contains sensitive security information and should be treated as confidential.
Distribution should be limited to authorized personnel only.

Table of Contents

1. Executive Summary

Assessment Overview

Our comprehensive security analysis has evaluated the HTTP security headers implementation for **https://cyberalphas.com**. This automated assessment identified critical security gaps that require immediate attention to protect against common web vulnerabilities.

Key Findings:

- Overall Security Score: **63/100**
- Risk Classification: ■ **Medium**
- Total Security Recommendations: **14**
- High-Priority Actions: **5**

Business Impact

The identified vulnerabilities expose your organization to potential security breaches, including cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks. Immediate implementation of our recommendations will significantly strengthen your security posture and protect sensitive user data.

Next Steps

We recommend prioritizing the high-risk findings detailed in Section 3 and implementing the security recommendations in order of priority. Our team is available to assist with remediation efforts and ongoing security monitoring.

2. Priority Findings Quick Reference

The following table summarizes the highest priority security findings that require immediate attention:

Priority	Finding	Severity	Action Require
#1	Add missing security header: x-content-type-options	HIGH	Immediate
#2	Add missing security header: x-frame-options	HIGH	Immediate
#3	Add missing security header: strict-transport-security	HIGH	Immediate
#4	Add missing security header: x-xss-protection	MEDIUM	Soon
#5	Add missing security header: referrer-policy	MEDIUM	Soon

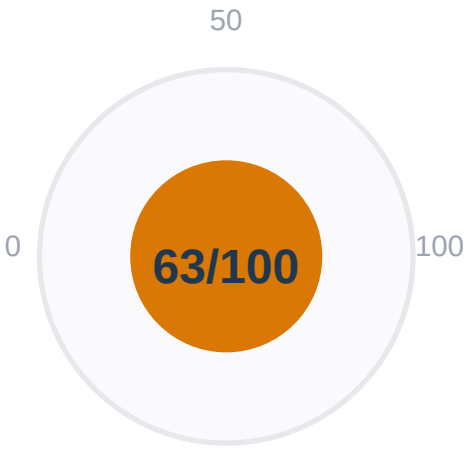
3. Scan Overview & Metrics

5.1 Scan Details

Property	Value
Target URL	https://cyberalphas.com
Scan Date	August 15, 2025 at 01:03 AM UTC
Security Score	63/100
Risk Level	■ Medium

Total Findings	14

5.2 Security Score Visualization

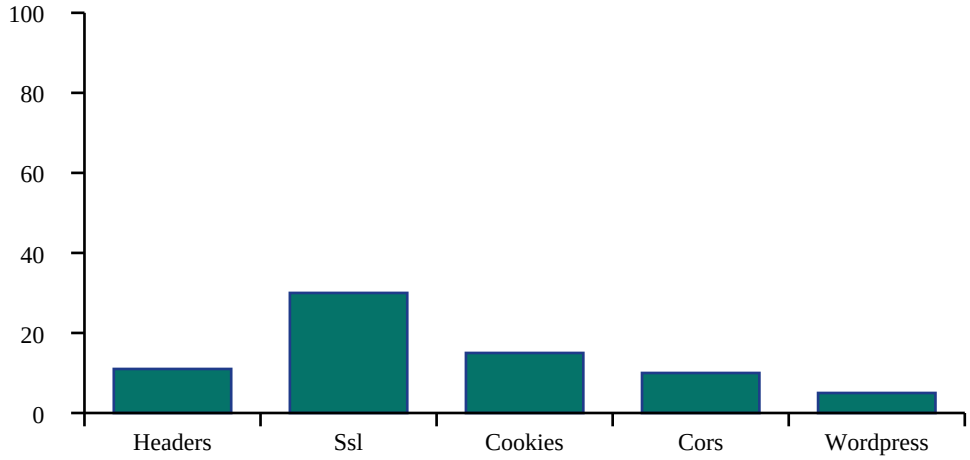


5.3 Security Category Analysis

The following analysis shows performance across different security categories:

Security Category	Score	Rating	Status
Headers	11/100	Poor	✗
Ssl	30/100	Poor	✗
Cookies	15/100	Poor	✗
Cors	10/100	Poor	✗
Wordpress	5/100	Poor	✗

Security Category Scores



4. Detailed Security Findings

6.1 Critical Missing Security Headers

The following essential security headers are missing and must be implemented immediately:

- **x-content-type-options** - Critical security header not implemented

Impact: Missing x-content-type-options exposes users to security vulnerabilities

Recommendation: Implement x-content-type-options with appropriate security policies

- **x-frame-options** - Critical security header not implemented

Impact: Missing x-frame-options exposes users to security vulnerabilities

Recommendation: Implement x-frame-options with appropriate security policies

- **strict-transport-security** - Critical security header not implemented

Impact: Missing strict-transport-security exposes users to security vulnerabilities

Recommendation: Implement strict-transport-security with appropriate security policies

• **x-xss-protection** - Critical security header not implemented

Impact: Missing x-xss-protection exposes users to security vulnerabilities

Recommendation: Implement x-xss-protection with appropriate security policies

• **referrer-policy** - Critical security header not implemented

Impact: Missing referrer-policy exposes users to security vulnerabilities

Recommendation: Implement referrer-policy with appropriate security policies

• **permissions-policy** - Critical security header not implemented

Impact: Missing permissions-policy exposes users to security vulnerabilities

Recommendation: Implement permissions-policy with appropriate security policies

• **cross-origin-opener-policy** - Critical security header not implemented

Impact: Missing cross-origin-opener-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-opener-policy with appropriate security policies

• **cross-origin-embedder-policy** - Critical security header not implemented

Impact: Missing cross-origin-embedder-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-embedder-policy with appropriate security policies

• **cross-origin-resource-policy** - Critical security header not implemented

Impact: Missing cross-origin-resource-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-resource-policy with appropriate security policies

6.2 Deprecated Security Headers

The following deprecated headers should be removed to prevent information disclosure:

• **server** - Deprecated header revealing server information

Impact: Information disclosure may aid attackers in reconnaissance

Recommendation: Remove or replace server with modern alternatives

6.3 Content Security Policy Vulnerabilities

Critical Content Security Policy configuration issues:

- CSP missing important directive: default-src

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: script-src

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: object-src

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: base-uri

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

5. Security Recommendations

The following recommendations are prioritized by security impact. Address high-priority items first:

1. ■ HIGH Add missing security header: x-content-type-options
2. ■ HIGH Add missing security header: x-frame-options
3. ■ HIGH Add missing security header: strict-transport-security
4. ■ HIGH Add missing security header: x-xss-protection
5. ■ HIGH Add missing security header: referrer-policy
6. ■ MEDIUM Add missing security header: permissions-policy
7. ■ MEDIUM Add missing security header: cross-origin-opener-policy
8. ■ MEDIUM Add missing security header: cross-origin-embedder-policy
9. ■ MEDIUM Add missing security header: cross-origin-resource-policy
10. ■ MEDIUM Remove deprecated header: server
11. ■ LOW CSP issue: CSP missing important directive: default-src
12. ■ LOW CSP issue: CSP missing important directive: script-src
13. ■ LOW CSP issue: CSP missing important directive: object-src
14. ■ LOW CSP issue: CSP missing important directive: base-uri

6. Expert AI Security Analysis

• *1. Executive Summary**

The security scan of cyberalphas.com reveals a medium-risk security posture (score of 63/100). The primary vulnerabilities stem from the absence of several crucial security headers, resulting in significant exposure to various attacks including Cross-Site Scripting (XSS), Clickjacking, and data breaches. While the SSL/TLS configuration appears sound, the lack of robust HTTP security headers significantly weakens the overall security profile of the website. Immediate action is required to address these deficiencies.

• *2. Critical Vulnerabilities**

The most critical vulnerabilities are the missing security headers. These headers are fundamental to mitigating common web attack vectors:

• **Missing `x-content-type-options`:** This header prevents MIME-sniffing attacks, which can lead to XSS vulnerabilities.
• **Missing `x-frame-options`:** This header helps prevent clickjacking attacks, where malicious websites embed the target website within an iframe to deceive users.
• **Missing `strict-transport-security` (HSTS):** This header enforces HTTPS connections, preventing man-in-the-middle attacks.
• **Missing other crucial headers:** The absence of `x-xss-protection`, `referrer-policy`, `permissions-policy`, `cross-origin-opener-policy`, `cross-origin-embedder-policy`, and `cross-origin-resource-policy` further weakens the site's defenses against various attack vectors.

The presence of a Content-Security-Policy (CSP) header is positive, but its incomplete configuration (missing crucial directives like `default-src`, `script-src`, `object-src`, and `base-uri`) severely limits its effectiveness. The deprecated `server` header should also be removed as it reveals unnecessary server information to potential attackers.

• *3. Security Header Analysis**

The analysis shows a significant lack of crucial HTTP security headers. While a CSP header is present, it's incomplete and therefore provides only limited protection. The missing headers expose the website to a wide range of attacks. The presence of the deprecated `server` header represents a minor vulnerability, revealing server details.

• *4. WordPress-Specific Risks (if applicable)**

The scan report indicates no specific WordPress vulnerabilities. However, the underlying security deficiencies could still impact a WordPress site, especially if themes or plugins aren't adequately secured.

• *5. SSL/TLS Configuration Review**

The SSL/TLS configuration appears satisfactory. The absence of weak cipher suites and the disabling of TLS compression are positive aspects.

• *6. Actionable Recommendations**

• **Implement Missing Security Headers:** Immediately add all the missing security headers (`x-content-type-options`, `x-frame-options`, `strict-transport-security`, `x-xss-protection`, `referrer-policy`, `permissions-policy`, `cross-origin-opener-policy`, `cross-origin-embedder-policy`, `cross-origin-resource-policy`). Consult online resources for proper configuration values.
• **Configure a Comprehensive CSP:** Thoroughly configure the CSP header, including `default-src`, `script-src`, `object-src`, and `base-uri` directives to restrict the sources allowed to load scripts, objects, and base URLs, minimizing the risk of XSS attacks.
• **Remove Deprecated Header:** Remove the deprecated `server` header.
• **Regular Security Scanning:** Conduct regular security scans using automated tools to proactively identify and address vulnerabilities.
• **Vulnerability Management:** Implement a robust vulnerability management process to track, prioritize, and remediate identified security issues promptly.
• **Web Application Firewall (WAF):** Consider implementing a WAF to provide an additional layer of protection against various web attacks.

• *7. Overall Risk Assessment**

The website currently faces a **medium-to-high risk** due to the significant lack of essential security headers. The missing headers expose the website to a wide range of attacks, potentially leading to data breaches, website defacement, and other serious security incidents. The immediate implementation of the recommended actions is crucial to mitigate these risks and improve the overall security posture of cyberalphas.com. Failure to address these issues could result in significant financial and reputational damage.

7. Methodology & Disclaimer

Assessment Methodology

This security assessment was conducted using automated scanning techniques that analyze HTTP response headers for security configurations. Our analysis includes:

• Evaluation of essential security headers (HSTS, CSP, X-Frame-Options, etc.)
• Detection of deprecated or information-leaking headers

- Content Security Policy validation and vulnerability assessment
- SSL/TLS configuration analysis
- Cookie security evaluation
- CORS policy review

Limitations & Disclaimer

This automated assessment provides a comprehensive overview of HTTP security header implementation but does not constitute a complete security audit. For thorough security assurance, we recommend:

- Manual penetration testing
- Code review and vulnerability assessment
- Infrastructure security evaluation
- Social engineering assessments

Important Notice: This report is confidential and intended solely for the organization that requested the assessment. The findings and recommendations should be implemented by qualified security professionals.

Thank You

Thank you for choosing **CyberHeaders Security** for your security assessment needs. We are committed to helping organizations strengthen their security posture through comprehensive analysis and actionable recommendations.

This automated assessment provides valuable insights into your HTTP security headers configuration. For a more comprehensive security evaluation, we recommend conducting additional penetration testing and manual security reviews.

Contact Information

Contact Type	Details
Technical Support	Email: security@cyberheaders.com Phone: +1 (555) 123-4567
Business Inquiries	Email: sales@cyberheaders.com Phone: +1 (555) 765-4321
Website	https://www.cyberheaders.com
Address	CyberHeaders Security 123 Security Boulevard Cyber City, CC 12345 United States

Follow-up Services Available

- **Detailed penetration testing** - Comprehensive security assessment
- **Security architecture review** - Infrastructure and design analysis
- **Compliance assessments** - Regulatory compliance verification
- **Security training and awareness** - Staff education programs
- **Incident response planning** - Emergency response preparation

Contact us to discuss how we can further enhance your security posture.